

CLAIMS

1. An apparatus having a digital protection mechanism, comprising:
 - a tangible object;
 - a digital protection system attached to said tangible object, said digital protection system comprising:
 - (a) an external interface for receiving data requests;
 - (b) a processor coupled to said external interface, said processor capable of transforming data according to a first public/private key encryption algorithm; and
 - (c) an internal data storage, said internal data storage storing an identity private key, said identity private key being inaccessible outside said external interface; and
 - a data descriptor associated with said digital protection system, said data descriptor including an identity public key, attribute data and a digital signature;wherein said processor performs a first transformation of data responsive to a request received through said external interface, said processor performing said first transformation of said data according to said first public/private key encryption algorithm using said identity private key, wherein a second transformation of data according to said first public/private key encryption algorithm using said identity public key is a complementary transformation of said first transformation.
2. The apparatus of claim 1, wherein said digital signature is an encryption of data derived from said identity public key and attribute data, said encryption being according to a second public/private key encryption algorithm using a signature private key, said digital signature being capable of decoding according to said second public/private key encryption algorithm using a signature public key.
3. The apparatus of claim 2, wherein said digital signature is an encryption of data derived from said identity public key and attribute data by performing a pre-defined hash function.

1 4. The apparatus of claim 1, wherein said digital protection system is implemented in
2 digital logic contained on a single integrated circuit substrate.

1 5. The apparatus of claim 4, wherein said data descriptor is stored in said internal
2 data storage contained on said single integrated circuit substrate.

1 6. The apparatus of claim 1, wherein at least a portion of said data descriptor is
2 stored in data storage external to said external interface of said digital protection system.

1 7. The apparatus of claim 1, wherein said tangible object is a digital data processing
2 device having at least one processor external to said digital protection system, said
3 processor external to said digital protection system communicating with said digital
4 protection system across said interface.

1 8. The apparatus of claim 1, wherein said external interface mates with a
2 corresponding interface of a digital data processing device separate from said tangible
3 object.

1 9. The apparatus of claim 1, wherein at least a portion of said attribute data is
2 encrypted.

1 10. A method for using verified information concerning a tangible object, comprising
2 the steps of:

3 accessing descriptor data associated with the tangible object, said descriptor data
4 including an identity public key for transforming data according to a first public/private
5 key encryption algorithm, attribute data containing information concerning said tangible
6 object, and a digital signature;

7 verifying that said digital signature matches said identity public key and said
8 attribute data;

9 performing a pair of complementary data transformations on source test data to
10 produce resultant test data, said pair of complementary data transformations being
11 performed by:

12 (a) performing a first data transformation according to said first public/private key
13 encryption algorithm using said identity public key, and

14 (b) accessing a digital protection system attached to said tangible object to perform
15 a second data transformation according to said first public/private key encryption
16 algorithm using an identity private key in said digital protection system, said identity
17 private key corresponding to said identity public key according to said first public/private
18 key encryption algorithm, said second data transformation being complementary to said
19 first data transformation;

20 comparing said source test data with said resultant test data; and

21 using said attribute data in a manner dependent on the results of said step of
22 verifying that said digital signature matches said identity public key and said attribute data,
23 and said step of comparing said source test data with said resultant test data.

1 11. The method for using verified information concerning a tangible object of claim 10,
2 wherein said digital signature represents an encryption of data derived from said identity
3 public key and said attribute data according to a derivation algorithm, said encryption
4 being according to a second public/private key encryption algorithm using a signature
5 private key, and wherein said step of verifying that said digital signature matches said
6 identity public key and said attribute data comprises:

7 decrypting said digital signature according to said second public/private key
8 encryption algorithm using a signature public key;

9 deriving data from said identity public key and said attribute data using said
10 derivation algorithm; and

11 comparing the decrypted digital signature to the data derived from said identity
12 public key and said attribute data according to said derivation algorithm.

13 12. The method for using verified information concerning a tangible object of claim 11,
14 wherein said derivation algorithm comprises a hash function.

15 13. The method for using verified information concerning a tangible object of claim 11,
16 wherein said derivation algorithm is an identity function which produces as output an
17 identical copy of the input.

18 14. The method for using verified information concerning a tangible object of claim 10,
19 wherein said first data transformation is an encryption of said source test data and said
20 second data transformation is a decryption of said source test data encrypted by said first
21 data transformation, said first data transformation being performed before said second
22 data transformation.

1 15. The method for using verified information concerning a tangible object of claim 10,
2 wherein said second data transformation is an encryption of said source test data and said
3 first data transformation is a decryption of said source test data encrypted by said second
4 data transformation, said second data transformation being performed before said first
5 data transformation.

1 16. The method for using verified information concerning a tangible object of claim 10,
2 wherein said step of accessing descriptor data comprises obtaining said descriptor data
3 from said digital protection system.

1 17. The method for using verified information concerning a tangible object of claim 10,
2 wherein said source test data is randomly generated data.

1 18. The method for using verified information concerning a tangible object of claim 10,
2 wherein said tangible object is a digital data processing device having at least one
3 processor external to said digital protection system.

1 19. The method for using verified information concerning a tangible object of claim 10,
2 wherein said digital protection system of said tangible object includes a coupling for
3 mating with a local digital data processing device separate from said tangible object.

1 20. A program product for using verified information concerning a tangible object,
2 said program product comprising a plurality of processor executable instructions recorded
3 on signal-bearing media, wherein said instructions, when executed by a processor of a
4 digital data processing device, cause the digital data processing device to perform the
5 steps of:

6 accessing descriptor data associated with the tangible object, said descriptor data
7 including an identity public key for transforming data according to a first public/private
8 key encryption algorithm, attribute data containing information concerning said tangible
9 object, and a digital signature;

10 verifying that said digital signature matches said identity public key and said
11 attribute data;

12 performing a pair of complementary data transformations on source test data to
13 produce resultant test data, said pair of complementary data transformations being
14 performed by:

15 (a) performing a first data transformation according to said first public/private key
16 encryption algorithm using said identity public key, and

17 (b) accessing a digital protection system attached to said tangible object to perform
18 a second data transformation according to said first public/private key encryption
19 algorithm using an identity private key in said digital protection system, said identity
20 private key corresponding to said identity public key according to said first public/private
21 key encryption algorithm, said second data transformation being complementary to said
22 first data transformation;

23 comparing said source test data with said resultant test data; and

24 using said attribute data in a manner dependent on the results of said step of
25 verifying that said digital signature matches said identity public key and said attribute data,
26 and said step of comparing said source test data with said resultant test data.

1 21. The program product for using verified information concerning a tangible object of
2 claim 20, wherein said digital signature represents an encryption of data derived from said
3 identity public key and said attribute data according to a derivation algorithm, said
4 encryption being according to a second public/private key encryption algorithm using a
5 signature private key, and wherein said step of verifying that said digital signature matches
6 said identity public key and said attribute data comprises:

7 decrypting said digital signature according to said second public/private key
8 encryption algorithm using a signature public key;

9 deriving data from said identity public key and said attribute data using said
10 derivation algorithm; and

11 comparing the decrypted digital signature to the data derived from said identity
12 public key and said attribute data according to said derivation algorithm.

1 22. The program product for using verified information concerning a tangible object of
2 claim 21, wherein said derivation algorithm comprises a hash function.

1 23. The program product for using verified information concerning a tangible object of
2 claim 21, wherein said derivation algorithm is an identity function which produces as
3 output an identical copy of the input.

1 24. The program product for using verified information concerning a tangible object of
2 claim 20, wherein said first data transformation is an encryption of said source test data
3 and said second data transformation is a decryption of said source test data encrypted by
4 said first data transformation, said first data transformation being performed before said
5 second data transformation.

1 25. The program product for using verified information concerning a tangible object of
2 claim 20, wherein said second data transformation is an encryption of said source test data
3 and said first data transformation is a decryption of said source test data encrypted by said
4 second data transformation, said second data transformation being performed before said
5 first data transformation.

1 26. The program product for using verified information concerning a tangible object of
2 claim 20, wherein said step of accessing descriptor data comprises obtaining said
3 descriptor data from said digital protection system.

1 27. The program product for using verified information concerning a tangible object of
2 claim 20, wherein said source test data is randomly generated data.

1 28. A method for updating attribute data associated with a tangible object, comprising
2 the steps of:

3 receiving a request to a service provider from a requestor to update said attribute
4 data, the request including an identity public key for transforming data according to a first
5 public/private key encryption algorithm;

6 performing a pair of complementary data transformations of source test data to
7 produce resultant test data, a first of said pair of complementary data transformations
8 being performed by said service provider according to said first public/private key
9 encryption algorithm using said identity public key, and a second of said pair of
10 complementary data transformations being performed by requesting a digital protection
11 system attached to said tangible object to perform said second data transformation
12 according to said first public/private key encryption algorithm using an identity private key
13 in said digital protection system, said identity private key corresponding to said identity
14 public key according to said first public/private key encryption algorithm;

15 comparing said source test data with said resultant test data, said comparing step
16 being performed by said service provider; and

17 depending on the results of said step of comparing said source test data with said
18 resultant test data, generating an updated descriptor, said updated descriptor comprising
19 said identity public key, updated attribute data, and a digital signature of said identity
20 public key and said updated attribute data.

1 29. The method for updating attribute data of claim 28, wherein said step of
2 generating an updated descriptor comprises generating said digital signature by encrypting
3 a derivation of said identity public key and said updated attribute data according to a
4 second public/private key encryption algorithm using a signature private key.

1 30. The method for updating attribute data of claim 28, wherein said request to update
2 attribute data includes old attribute data and an old digital signature, said old digital
3 signature representing an encryption of data derived from said identity public key and said
4 old attribute data, said encryption being according to a second public/private key
5 encryption algorithm using a signature private key, said method further comprising:

6 decrypting said old digital signature according to said second public/private key
7 encryption algorithm using a signature public key;

8 comparing the decrypted old digital signature to said data derived from said
9 identity public key and said old attribute data to verify said attribute data;

10 wherein said step of generating an updated descriptor further depends on the
11 results of said step of comparing the decrypted old digital signature to said data derived
12 for said identity public key and said old attribute data.

1 31. The method for updating attribute data of claim 28, wherein said first of said pair
2 of complementary data transformations is an encryption of said source test data and said
3 second of said pair of complementary data transformations is a decryption of said source
4 test data encrypted by said first transformation, said first transformation being performed
5 before said second transformation.

1 32. The method for updating attribute data of claim 28, wherein said second of said
2 pair of complementary data transformations is an encryption of said source test data and
3 said first of said pair of complementary data transformations is a decryption of said source
4 test data encrypted by said second transformation, said second transformation being
5 performed before said first transformation.

1 33. The method for updating attribute data of claim 28, wherein said service provider
2 is remote from said tangible object.

1 34. The method for updating attribute data of claim 33, wherein said tangible object is
2 coupled to a local device, said local device communicating remotely with said service
3 provider.

1 35. The method for updating attribute data of claim 28, further comprising the step of
2 accessing a database in said service provider to verify that the requestor is entitled to the
3 requested update.

1 36. The method for updating attribute data of claim 28, wherein said source test data
2 is randomly generated data.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208

1 37. A method for using verified information concerning a tangible object, comprising
2 the steps of:

3 accessing descriptor data associated with the tangible object, said descriptor data
4 including an identity public key for transforming data according to a first public/private
5 key encryption algorithm, attribute data containing information concerning said tangible
6 object, and a digital signature, wherein said digital signature represents an encryption of
7 data derived from said identity public key and said attribute data according to a derivation
8 algorithm, said encryption being according to a second public/private key encryption
9 algorithm using a signature private key;

10 decrypting said digital signature according to said second public/private key
11 encryption algorithm using a signature public key;

12 deriving data from said identity public key and said attribute data using said
13 derivation algorithm;

14 comparing the decrypted digital signature to the data derived from said identity
15 public key and said attribute data according to said derivation algorithm;

16 generating random source test data;

17 performing a pair of complementary data transformations of said source test data
18 to produce resultant test data, including:

19 (a) performing a first data transformation of said pair of complementary
20 data transformations according to said first public/private key encryption algorithm
21 using said identity public key, and

22 (b) accessing a digital protection system attached to said tangible object to
23 perform a second data transformation of said pair of complementary data
24 transformations, said second data transformation being according to said first
25 public/private key encryption algorithm using an identity private key in said digital
26 protection system, said identity private key corresponding to said identity public
27 key according to said first public/private key encryption algorithm;
28 comparing said random source test data with said resultant test data; and
29 using said attribute data in a manner dependent on the results of said step of

30 comparing the decrypted digital signature to the data derived from said identity public key
31 and said attribute data, and said step of comparing said random source test data with said
32 resultant test data.

1 38. The method for using verified information concerning a tangible object of claim 37,
2 wherein said first data transformation is an encryption of said source test data and said
3 second data transformation is a decryption of said source test data encrypted by said first
4 data transformation, said first data transformation being performed before said second
5 data transformation..

1 39. The method for using verified information concerning a tangible object of claim 37,
2 wherein said second data transformation is an encryption of said source test data and said
3 first data transformation is a decryption of said source test data encrypted by said second
4 data transformation, said second data transformation being performed before said first
5 data transformation.

1 40. The method for using verified information concerning a tangible object of claim 37,
2 wherein said step of accessing descriptor data comprises obtaining said descriptor data
3 from said digital protection system.

1 41. The method for using verified information concerning a tangible object of claim 37,
2 wherein said derivation algorithm comprises a hash function.

1 42. The method for using verified information concerning a tangible object of claim 41,
2 wherein said hash function belongs to the set consisting of SHA-1 and MD5.

1 43. The method for using verified information concerning a tangible object of claim 37,
2 wherein said digital protection system is implemented in digital logic contained on a single
3 integrated circuit substrate.

1 44. An apparatus for verifying information concerning a tangible object, comprising:
2 a programmable processor;
3 a memory for storing instructions executable on said programmable processor;
4 a digital protection system interface coupled to said processor, said interface
5 communicating with a digital protection system for said tangible object;
6 a protection system verification program executable on said programmable
7 processor, wherein said protection system verification program
8 (a) obtains a data descriptor from a said digital protection system through
9 said interface, said data descriptor comprising an identity public key for
10 transforming data according to a first public/private key encryption algorithm,
11 attribute data containing information concerning said object, and a digital
12 signature;
13 (b) verifies that said digital signature matches said identity public key and
14 said attribute data;
15 (c) performs a first data transformation of a pair of complementary data
16 transformations of source test data which produce resultant test data, said first
17 data transformation being according to said first public/private key encryption
18 algorithm using said identity public key;
19 (d) directs said digital protection system to perform a second data
20 transformation of said pair of complementary data transformations of source test
21 data which produce resultant test data, said second data transformation being
22 complementary to said first data transformation;
23 (e) compares said source test data with said resultant test data; and
24 (f) verifies information concerning the tangible object responsive to steps
25 (b) and (e).

1 45. The apparatus for verifying information concerning a tangible object of claim 44,
2 wherein said digital protection system interface is a physical coupling which supplies
3 power to said digital protection system.

1 46. The apparatus for verifying information concerning a tangible object of claim 44,
2 wherein said digital protection system interface is a remote transmission interface.

1 47. The apparatus for verifying information concerning a tangible object of claim 44,
2 wherein said digital signature represents an encryption of data derived from said identity
3 public key and said attribute data according to a derivation algorithm, said encryption
4 being according to a second public/private key encryption algorithm using a signature
5 private key, and wherein said protection system verification program verifies that said
6 digital signature matches said identity public key and said attribute data by:

7 decrypting said digital signature according to said second public/private key
8 encryption algorithm using a signature public key;

9 deriving data from said identity public key and said attribute data using said
10 derivation algorithm; and

11 comparing the decrypted digital signature to the data derived from said identity
12 public key and said attribute data according to said derivation algorithm.

1 48. The apparatus for verifying information concerning a tangible object of claim 44,
2 wherein said first data transformation is an encryption of said source test data and said
3 second data transformation is a decryption of said source test data encrypted by said first
4 data transformation, said first data transformation being performed before said second
5 data transformation..

1 49. The apparatus for verifying information concerning a tangible object of claim 44,
2 wherein said second data transformation is an encryption of said source test data and said
3 first data transformation is a decryption of said source test data encrypted by said second
4 data transformation, said second data transformation being performed before said first
5 data transformation.

1 50. The apparatus for verifying information concerning a tangible object of claim 44,
2 wherein said source test data is randomly generated data.

1 51. A method for verifying the identity of a tangible object, comprising the steps of:
2 accessing a descriptor associated with the tangible object, said descriptor including
3 an identity public key for transforming data according to a first public/private key
4 encryption algorithm;

5 providing source test data;

6 performing a pair of complementary data transformations on said source test data
7 to produce resultant test data, said pair of complementary data transformations being
8 performed by:

9 (a) performing a first data transformation according to said first public/private key
10 encryption algorithm using said identity public key, and

11 (b) accessing a digital protection system attached to said tangible object to perform
12 a second data transformation according to said first public/private key encryption
13 algorithm using an identity private key in said digital protection system, said identity
14 private key corresponding to said identity public key according to said first public/private
15 key encryption algorithm, said second data transformation being complementary to said
16 first data transformation;

17 comparing said source test data with said resultant test data; and

18 using said descriptor to identify said tangible object dependent on the results of
19 said step of comparing said source test data with said resultant test data.

1 52. The method for verifying the identity of a tangible object of claim 51, wherein said
2 step of using said descriptor to identify said tangible object comprises using said public
3 identity key to access identifying information in a database.

1 53. The method for verifying the identity of a tangible object of claim 51, wherein said
2 descriptor comprises attribute data and a digital signature of said identity public key and
3 said attribute data, and wherein said step of using said descriptor to identify said tangible
4 object comprises using said attribute data to identify said tangible object if said digital
5 signature matches said identity public key and said attribute data.

1 54. The method for verifying the identity of a tangible object of claim 51, wherein said
2 first data transformation is an encryption of said source test data and said second data
3 transformation is a decryption of said source test data encrypted by said first data
4 transformation, said first data transformation being performed before said second data
5 transformation..

1 55. The method for verifying the identity of a tangible object of claim 51, wherein said
2 second data transformation is an encryption of said source test data and said first data
3 transformation is a decryption of said source test data encrypted by said second data
4 transformation, said second data transformation being performed before said first data
5 transformation.

1 56. A method for providing telephone service, comprising the steps of:
2 transmitting an identity public key from a telephone to a service provider;
3 providing source test data, said step of providing source test data being performed
4 by said service provider;
5 performing a pair of complementary data transformations of said source test data
6 to produce resultant test data, by:
7 (a) performing a first data transformation of said pair of complementary
8 data transformations according to a first public/private key encryption algorithm
9 using said identity public key, said performing a first data transformation step
10 being performed by said service provider, and
11 (b) requesting said telephone to perform a second data transformation of
12 said pair of complementary data transformations according to said first
13 public/private key encryption algorithm using an identity private key stored in said
14 telephone, and receiving the results of said second data transformation;
15 comparing said source test data to said resultant test data, said comparing step
16 being performed by said service provider;
17 providing service to said telephone depending on whether said source test data
18 matches said resultant test data.

1 57. The method for providing telephone service of claim 56, further comprising the
2 steps of:
3 transmitting, from said telephone to said service provider, attribute data and a
4 digital signature of said identity public key and said attribute data;
5 verifying that said digital signature matches said identity public key and said
6 attribute data; and
7 providing service to said telephone depending on whether said digital signature
8 matches said identity public key and said attribute data.

1 58. The method for providing telephone service of claim 57, wherein said digital
2 signature representing an encryption of data derived from said identity public key and said
3 attribute data, said encryption being according to a second public/private key encryption
4 algorithm using a signature private key, and wherein said step of verifying that said digital
5 signature matches said identity public key and said attribute data comprises:

6 decrypting said digital signature according to said second public/private key
7 encryption algorithm using a signature public key;

8 comparing the decrypted digital signature to said data derived from said identity
9 public key and said attribute data to verify said attribute data..

1 59. The method for providing telephone service of claim 57, wherein said attribute
2 data includes an identifier identifying said telephone.

1 60. The method for providing telephone service of claim 59, wherein said identifier
2 comprises a telephone number of said telephone.

1 61. The method for providing telephone service of claim 56, wherein said first data
2 transformation is an encryption of said source test data and said second data
3 transformation is a decryption of said source test data encrypted by said first data
4 transformation, said first data transformation being performed before said second data
5 transformation..

1 62. The method for providing telephone service of claim 56, wherein said second data
2 transformation is an encryption of said source test data and said first data transformation is
3 a decryption of said source test data encrypted by said second data transformation, said
4 second data transformation being performed before said first data transformation.

1 63. The method for providing telephone service of claim 56, wherein said telephone is
2 a cellular telephone.

1 64. The method for providing telephone service of claim 56, wherein said source test
2 data is randomly generated data.

1 65. A telephone, comprising:
2 a transceiver for communicating with a service provider;
3 a telephonic interface for audible communication with a user;
4 an identity public key and corresponding identity private key according to a first
5 public/private key encryption algorithm;
6 a digital controller controlling the operation of said telephone, wherein said
7 controller:

8 (a) causes said telephone to transmit said identity public key to a service
9 provider with a request for service;

10 (b) responsive to a request from said service provider, performs a data
11 transformation of test data received from said service provider according to said
12 first public/private key encryption algorithm using said identity private key; and

13 (c) transmits the transformed test data to said service provider.

1 66. The telephone of claim 65, further comprising a digital protection system, said
2 digital protection system comprising:

3 (a) an external interface for receiving data requests;

4 (b) an internal processor coupled to said external interface, said processor capable
5 of performing said data transformation according to said first public/private key
6 encryption algorithm; and

7 (c) an internal data storage;

8 wherein said identity private key is stored in said internal data storage within said digital
9 protection system, said identity private key being inaccessible outside said external
10 interface to said digital protection system.

1 67. The telephone of claim 66, wherein said digital protection system is implemented
2 in digital logic contained on a single integrated circuit substrate.

1 68. The telephone of claim 65, further comprising attribute data and a digital signature
2 of said attribute data and said identity public key, wherein said digital controller further
3 causes said telephone to transmit said attribute data and said digital signature to said
4 service provider with a request for service.

1 69. The telephone of claim 68, wherein said digital signature represents an encryption
2 of data derived from said identity public key and said attribute data, said encryption being
3 according to a second public/private key encryption algorithm using a signature private
4 key.

1 70. The telephone of claim 68, wherein said attribute data includes an identifier
2 identifying said telephone.

1 71. A method in a telephone service provider for updating attribute data contained in a
2 telephone, comprising the steps of:

3 obtaining a descriptor associated with said telephone, said descriptor including an
4 identity public key for transforming data according to a first public/private key encryption
5 algorithm, attribute data, and a digital signature;

6 verifying that said digital signature matches said attribute data and said identity
7 public key;

8 performing a pair of complementary data transformations of source test data to
9 produce resultant test data, a first of said pair of complementary data transformations
10 being performed by said service provider according to said first public/private key
11 encryption algorithm using said identity public key, and a second of said pair of
12 complementary data transformations being performed by requesting said telephone to
13 perform said second data transformation according to said first public/private key
14 encryption algorithm using an identity private key in said telephone and receiving data
15 from said telephone responsive to said request, said identity private key corresponding to
16 said identity public key according to said first public/private key encryption algorithm;

17 comparing said source test data with said resultant test data;

18 depending on the results of said step of comparing said source test data with said
19 resultant test data, generating an updated descriptor, said updated descriptor comprising
20 said identity public key, updated attribute data, and a digital signature of said identity
21 public key and said updated attribute data; and

22 transmitting said updated descriptor to said telephone.

1 72. The method in a telephone service provider for updating attribute data contained in
2 a telephone of claim 71, wherein said step of generating an updated descriptor comprises
3 generating said digital signature by encrypting a derivation of said identity public key and
4 said updated attribute data according to a second public/private key encryption algorithm
5 using a signature private key.

1 73. The method in a telephone service provider for updating attribute data contained in
2 a telephone of claim 71, wherein said first of said pair of complementary data
3 transformations is an encryption of said source test data and said second of said pair of
4 complementary data transformations is a decryption of said source test data encrypted by
5 said first transformation, said first transformation being performed before said second
6 transformation.

1 74. The method in a telephone service provider for updating attribute data contained in
2 a telephone of claim 71, wherein said second of said pair of complementary data
3 transformations is an encryption of said source test data and said first of said pair of
4 complementary data transformations is a decryption of said source test data encrypted by
5 said second transformation, said second transformation being performed before said first
6 transformation.

1 75. The method in a telephone service provider for updating attribute data contained in
2 a telephone of claim 71, wherein said source test data is randomly generated data.

3 76. The method in a telephone service provider for updating attribute data contained in
4 a telephone of claim 71, wherein said telephone is a cellular telephone.

1 77. A machine having multiple parts, comprising:
2 a first replaceable part
3 a digital controller controlling operation of at least one function of said machine,
4 said digital controller being external to said first replaceable part;
5 a digital protection system attached to said first replaceable part, said digital
6 protection system comprising:
7 (a) an external interface for receiving data requests,
8 (b) a processor coupled to said external interface, said processor capable
9 of performing a first data transformation according to a first public/private key
10 encryption algorithm, and
11 (c) an internal data storage, said internal data storage storing an identity
12 private key, said identity private key being inaccessible outside said external
13 interface; and
14 a data descriptor associated with said digital protection system, said data
15 descriptor including an identity public key, attribute data and a digital signature;
16 wherein said controller verifies information concerning said first replaceable part
17 by:
18 (a) obtaining said data descriptor associated with said digital protection
19 system,
20 (b) performing a second data transformation of test data according to said
21 first public/private key encryption algorithm using said identity public key, said
22 second data transformation being complementary to said first data transformation,
23 (c) accessing said digital protection system attached to said first replaceable
24 part to perform said first data transformation of said test data using said identity
25 private key,
26 (d) comparing data undergoing said first and second data transformations
27 to test data before transformation; and
28 (e) verifying that said data descriptor has not been altered using said digital
29 signature.

1 78. The machine of claim 77, wherein said digital signature is an encryption of data
2 derived from said identity public key and attribute data, said encryption being according to
3 a second public/private key encryption algorithm using a signature private key, and
4 wherein said controller verifies that said data descriptor has not been altered by:

5 (e1) decrypting said digital signature according to said second
6 public/private key encryption algorithm using a signature public key, and

7 (e2) comparing the decrypted digital signature to data derived from said
8 identity public key and said attribute data according to said derivation algorithm to
9 verify said descriptor data..

1 79. The machine of claim 77, wherein said first data transformation is an encryption of
2 said source test data and said second data transformation is a decryption of said source
3 test data encrypted by said first data transformation, said first data transformation being
4 performed before said second data transformation..

1 80. The machine of claim 77, wherein said second data transformation is an encryption
2 of said source test data and said first data transformation is a decryption of said source test
3 data encrypted by said second data transformation, said second data transformation being
4 performed before said first data transformation.

1 81. The machine of claim 77, wherein said apparatus comprises a plurality of
2 replaceable parts, at least some of which contain a respective digital protection system.

1 82. The machine of claim 81, wherein said machine is a motor vehicle.

1 83. The machine of claim 77, wherein said digital protection is implemented in digital
2 logic contained on a single integrated circuit substrate.

1 84. The machine of claim 83, wherein said data descriptor is stored in said internal
2 data storage contained on said single integrated circuit substrate.

1 85. The machine of claim 84, wherein said data descriptor contains a unique machine
2 identifier, said unique machine identifier distinguishing said machine from other machines
3 of the same type.

1 86. A replaceable part for a machine having multiple parts, comprising:
2 a part performing a function for said machine, and
3 a digital protection system attached to said part, said digital protection system
4 comprising:
5 (a) an external interface for communicating with a digital controller of said
6 machine, said digital controller being located externally to said replaceable part;
7 (b) a processor coupled to said external interface, said processor capable
8 of performing a data transformation according to a first public/private key
9 encryption algorithm, and
10 (c) an internal data storage, said internal data storage storing an identity
11 private key, said identity private key being inaccessible outside said external
12 interface, and a data descriptor, said data descriptor including an identity public
13 key, attribute data and a digital signature;
14 wherein, responsive to a request received through said external interface, said
15 processor of said digital protection system performs said data transformation according to
16 said first public/private key encryption algorithm using said identity private key.

1 87. The machine of claim 86, wherein said machine is a motor vehicle.

1 88. The replaceable part for a machine having multiple parts of claim 86, wherein said
2 digital signature is an encryption of data derived from said identity public key and attribute
3 data, said encryption being according to a second public/private key encryption algorithm
4 using a signature private key, said digital signature being capable of decoding according to
5 said second public/private key encryption algorithm using a signature public key.

1 89. The replaceable part for a machine having multiple parts of claim 88, wherein said
2 digital signature is an encryption of data derived from said identity public key and attribute
3 data by performing a pre-defined hash function.

1 90. The machine of claim 86, wherein said digital protection system is implemented in
2 digital logic contained on a single integrated circuit substrate.

1 91. A method of operating a machine having multiple parts, including a first
2 replaceable part having a digital protection system and a digital controller external to said
3 first replaceable part for controlling operation of said machine, said method comprising the
4 steps of:

5 (a) obtaining a data descriptor associated with said first replaceable part, said data
6 descriptor including an identity public key, attribute data, and a digital signature;

7 (b) performing a complementary pair of data transformations of source test data to
8 produce resultant test data, including a first data transformation performed by said digital
9 controller according to a first public/private key encryption algorithm using said identity
10 public key, and a second data transformation performed by said digital protection system,
11 said second data transformation being complementary to said first data transformation;

12 (c) comparing said source test data to said resultant test data;

13 (d) verifying that said data descriptor has not been altered using said digital
14 signature; and

15 (e) using the results of steps (c) and (d) in the operation of said machine.

1 92. The method of operating a machine of claim 91, wherein step (e) comprises
2 presenting information derived from the results of steps (c) and (d) to a user.

1 93. The method of operating a machine of claim 91, wherein step (e) comprises
2 selectively disabling at least one function of said machine responsive to the results of steps
3 (c) and (d).

1 94. The method of operating a machine of claim 91, wherein said data descriptor
2 contains a unique machine identifier, said unique machine identifier distinguishing said
3 machine from other machines of the same type, said method further comprising the step of
4 verifying that said unique machine identifier in said data descriptor matches a unique
5 machine identifier associated with said machine.

1 95. The method of operating a machine of claim 91, wherein said first data
2 transformation is an encryption of said source test data and said second data
3 transformation is a decryption of said source test data encrypted by said first data
4 transformation, said first data transformation being performed before said second data
5 transformation.

1 96. The method of operating a machine of claim 91, wherein said second data
2 transformation is an encryption of said source test data and said first data transformation is
3 a decryption of said source test data encrypted by said second data transformation, said
4 second data transformation being performed before said first data transformation.

1 97. A personal identity document for a subject, comprising:
2 a carrier; and
3 a digital protection system attached to said carrier, said digital protection system
4 comprising:
5 (a) an external interface for receiving data requests,
6 (b) a processor coupled to said external interface, said processor capable
7 of performing a data transformation according to a first public/private key
8 encryption algorithm, and
9 (c) an internal data storage, said internal data storage storing an identity
10 private key and a data descriptor, said identity private key being inaccessible
11 outside said external interface, said data descriptor including an identity public key,
12 attribute data and a digital signature of said identity public key and said attribute
13 data, said identity public key corresponding to said identity private key according
14 to said first public/private key encryption algorithm;
15 wherein said processor performs said data transformation of data responsive to a
16 request received through said external interface, said processor performing said data
17 transformation according to said first public/private key encryption algorithm using said
18 identity private key.

19 98. The personal identity document of claim 97, wherein said attribute data comprises
20 data identifying a digitized photographic image of said subject.

1 99. The personal identity document of claim 97, wherein said attribute data comprises
2 data identifying said subject according to at least one physical characteristic verified by a
3 digital data processing device.

1 100. The personal identity document of claim 99, wherein said data identifying a person
2 according to at least one physical characteristic comprises data derived from an iris scan.

3 101. The personal identity document of claim 99, wherein said data identifying a person

1 according to at least one physical characteristic comprises data derived from an retina
2 scan.

1 102. The personal identity document of claim 99, wherein said data identifying a person
2 according to at least one physical characteristic comprises data derived from a voice
3 sample.

1 103. The personal identity document of claim 97, wherein said digital signature is an
2 encryption of data derived from said identity public key and attribute data, said encryption
3 being according to a second public/private key encryption algorithm using a signature
4 private key, said digital signature being capable of decoding according to said second
5 public/private key encryption algorithm using a signature public key.

1 104. The personal identity document of claim 103, wherein said digital signature is an
2 encryption of data derived from said identity public key and attribute data by performing a
3 pre-defined hash function.

1 105. The apparatus of claim 97, wherein said digital protection system is implemented
2 in digital logic contained on a single integrated circuit substrate.

1 106. A control station for verifying the personal identities of multiple subjects,
2 comprising:
3 a programmable processor;
4 a memory, said memory storing a control program which executes on said
5 programmable processor and controls at least some operations of said control station;
6 a digital personal identity document interface, said interface communicating with
7 a digital personal identity document of a subject;
8 wherein said control program verifies a personal identity of a subject by:
9 (a) obtaining a data descriptor from said digital personal identity
10 document of the subject through said interface, said descriptor comprising an
11 identity public key for transforming data according to a first public/private key
12 encryption algorithm, attribute data containing identifying information concerning
13 said subject, and a digital signature;
14 (b) verifying that said digital signature matches said identity public key
15 and said attribute data;
16 (c) performing a pair of complementary data transformations of source test
17 data to produce resultant test data, said pair of complementary data
18 transformations including (i) a first data transformation according to said first
19 public/private key encryption algorithm using said identity public key, said first
20 data transformation being performed externally to said digital personal identity
21 document, and (ii) a second data transformation according to said first
22 public/private key encryption algorithm, said second data transformation being
23 performed by said digital personal identity document responsive to a request by
24 said control program;
25 (d) comparing said source test data with said resultant test data; and
26 (e) verifying the identity of said subject depending on the results of said
27 step of verifying that said digital signature matches said identity public key and
28 said attribute data, and said step of comparing said source test data with said
29 resultant test data.

1 107. The control station for verifying the identities of multiple subjects of claim 106,
2 wherein said control station is a passport control station at a jurisdictional entry or exit
3 location.

1 108. The control station for verifying the identities of multiple subjects of claim 106,
2 further comprising an operator interface displaying information to an operator, said
3 information including a result of steps (b) and (d).

1 109. The control station for verifying the identities of multiple subjects of claim 108,
2 wherein said information displayed to said operator further comprises at least some
3 identifying information derived from said attribute data..

1 110. The control station for verifying the identities of multiple subjects of claim 109,
2 wherein said identifying information derived from said attribute data comprises a
3 digitized photographic image of said subject.

1 111. The control station for verifying the identities of multiple subjects of claim 106,
2 further comprising a physical characteristic sensing device, said physical characteristic
3 sensing device automatically sensing at least one physical characteristic of the subject,
4 said at least one physical characteristic being compared to identifying data contained in
5 said data descriptor to verify the identity of said subject.

1 112. The control station for verifying the identities of multiple subjects of claim 111,
2 wherein said physical characteristic sensing device is an iris scanning device.

1 113. The control station for verifying the identities of multiple subjects of claim 106,
2 wherein said digital signature represents an encryption of data derived from said identity
3 public key and said attribute data according to a derivation algorithm, said encryption
4 being according to a second public/private key encryption algorithm using a signature
5 private key, and wherein said control program verifies that said digital signature matches
6 said identity public key and said attribute data by:

7 decrypting said digital signature according to said second public/private key
8 encryption algorithm using a signature public key;

9 deriving data from said identity public key and said attribute data using said
10 derivation algorithm; and

11 comparing the decrypted digital signature to the data derived from said identity
12 public key and said attribute data according to said derivation algorithm.

1 114. The control station for verifying the identities of multiple subjects of claim 106,
2 wherein said first data transformation is an encryption of said source test data and said
3 second data transformation is a decryption of said source test data encrypted by said first
4 data transformation, said first data transformation being performed before said second
5 data transformation.

1 115. The control station for verifying the identities of multiple subjects of claim 106,
2 wherein said second data transformation is an encryption of said source test data and said
3 first data transformation is a decryption of said source test data encrypted by said second
4 data transformation, said second data transformation being performed before said first
5 data transformation.

116. The control station for verifying the identities of multiple subjects of claim 106,
wherein said source test data is randomly generated data.

1 117. A method for verifying the identity of a subject, comprising the steps of:

2 (a) obtaining a data descriptor from a digital personal identity document of the
3 subject, said descriptor comprising an identity public key for transforming data according
4 to a first public/private key encryption algorithm, attribute data containing identifying
5 information concerning said subject, and a digital signature;

6 (b) verifying that said digital signature matches said identity public key and said
7 attribute data;

8 (c) performing a pair of complementary data transformations of source test data to
9 produce resultant test data, wherein a first data transformation of said pair is performed
10 by a verifying device according to said first public/private key encryption algorithm using
11 said identity public key, and wherein a second data transformation of said pair is
12 performed by said digital personal identity document responsive to a request from a
13 verifying device, said second data transformation being complementary to said first data
14 transformation;

15 (d) comparing said source test data with said resultant test data; and

16 (e) verifying the identity of said subject responsive to the results of steps (b) and
17 (d).

1 118. The method for verifying the identity of a subject of claim 117, wherein said
2 digital signature represents an encryption of data derived from said identity public key
3 and said attribute data according, said encryption being according to a second
4 public/private key encryption algorithm using a signature private key, and wherein step
5 (b) comprises the steps of:

6 decrypting said digital signature according to said second public/private key
7 encryption algorithm using a signature public key;

8 comparing the decrypted digital signature to said data derived from said identity
9 public key and said attribute data.

1 119. The method for verifying the identity of a subject of claim 118, wherein said
2 digital signature is an encryption of data derived from said identity public key and
3 attribute data by performing a pre-defined hash function.

1 120. The method for verifying the identity of a subject of claim 117, wherein said first
2 data transformation is an encryption of said source test data and said second data
3 transformation is a decryption of said source test data encrypted by said first data
4 transformation, said first data transformation being performed before said second data
5 transformation..

1 121. The method for verifying the identity of a subject of claim 117, wherein said
2 second data transformation is an encryption of said source test data and said first data
3 transformation is a decryption of said source test data encrypted by said second data
4 transformation, said second data transformation being performed before said first data
5 transformation.

1 122. The method for verifying the identity of a subject of claim 117, further comprising
2 the step of displaying information to an operator, said information including a result of
3 step (e).

1 123. The method for verifying the identity of a subject of claim 122, wherein said
2 information displayed to said operator further comprises at least some identifying
3 information derived from said attribute data..

1 124. The method for verifying the identity of a subject of claim 123, wherein said
2 identifying information derived from said attribute data comprises a digitized
3 photographic image of said subject.

1 125. The method for verifying the identity of a subject of claim 117, further comprising
2 the steps of:

3 automatically sensing at least one physical characteristic of the subject with a
4 sensing device; and

5 automatically comparing said at least one physical characteristic to identifying
6 data contained in said data descriptor to verify the identity of said subject.

1 126. The method for verifying the identity of a subject of claim 125, wherein said
2 sensing device is an iris scanning device.

1 127. The method for verifying the identity of a subject of claim 117, wherein said
2 source test data is randomly generated data.

1 128. A method for providing television service to a subscriber, comprising the steps of:
2 accessing descriptor data in a television receiving apparatus, said descriptor data
3 including an identity public key for transforming data according to a first public/private
4 key encryption algorithm, attribute data and a digital signature of said descriptor data;
5 verifying that said descriptor data has not been altered using said digital signature;
6 providing source test data;
7 performing a first data transformation of a pair of data transformations of said
8 source test data, said pair of data transformations producing resultant test data, said first
9 data transformation being according to said first public/private key encryption algorithm
10 using said identity public key;
11 requesting a digital protection system of said television receiving apparatus to
12 perform a second data transformation of said pair of data transformations of said source
13 test data, said digital protection system including
14 (a) a processor capable of performing said second data transformation according
15 to a first public/private key encryption algorithm; and
16 (b) a permanent data storage accessible only through said processor, said
17 permanent data storage storing an identity private key for performing said second
18 data transformation according to said first public/private key encryption
19 algorithm;
20 comparing said source test data with the resultant test data to verify the identity of
21 said digital protection system; and
22 using said attribute data to access one or more television channels on behalf of
23 said subscriber depending on the results of said verifying step and said comparing step.

1 129. The method for providing television service of claim 128, wherein said attribute
2 data comprises keys for accessing a plurality of channel signals.

1 130. The method for providing television service of claim 129, wherein said keys for
2 accessing a plurality of channel signals are encrypted.

1 131. The method for providing television service of claim 128, wherein said digital
2 signature represents an encryption of data derived from said identity public key and said
3 attribute data, said encryption being according to a second public/private key encryption
4 algorithm using a signature private key, said verifying step comprising:
5 decrypting said digital signature according to said second public/private key
6 encryption algorithm using a signature public key; and
7 comparing the decrypted digital signature to said data derived from said identity
8 public key and said attribute data to verify said descriptor data.

1 132. The method for providing television service of claim 128, wherein said first data
2 transformation is an encryption of said source test data and said second data
3 transformation is a decryption of said source test data encrypted by said first data
4 transformation, said first data transformation being performed before said second data
5 transformation..

1 133. The method for providing television service of claim 128, wherein said second
2 data transformation is an encryption of said source test data and said first data
3 transformation is a decryption of said source test data encrypted by said second data
4 transformation, said second data transformation being performed before said first data
5 transformation.

1 134. A television receiving system, comprising:
2 a digital controller controlling the operation of said television system;
3 a television signal transmission interface coupled to said digital controller, said
4 interface receiving television signals from an external source and transmitting television
5 signals to a display apparatus;
6 a digital protection system coupled to said digital controller, said digital protection
7 system securely storing an identity private key, and said digital protection system
8 performing a first data transformation according to a first public/private key encryption
9 algorithm in response to a command from said digital controller;
10 a data descriptor associated with said digital protection system, said data
11 descriptor including an identity public key for performing data transformations according
12 to said first public/private key encryption algorithm, attribute data and a digital signature;
13 wherein said controller:
14 (a) directs said digital protection system to perform said first data
15 transformation of test data;
16 (b) performs a second data transformation of test data according to said
17 first public/private key encryption algorithm using said identity public key;
18 (c) compares test data before transformation with test data after said first
19 and said second transformation,
20 (d) verifies that said digital signature matches said identity public key, and
21 (e) uses said attribute data to access television channels on behalf of a user
22 responsive to the results of steps (c) and (d).

1 135. The television receiving system of claim 134, wherein said television signal
2 transmission interface receives television signals from a satellite receiver.

1 136. The television receiving system of claim 134, wherein said attribute data
2 comprises keys for accessing a plurality of channel signals.

1 137.. The television receiving system of claim 136, wherein said keys for accessing a
2 plurality of channel signals are encrypted.

1 138. The television receiving system of claim 134, wherein said digital signature
2 represents an encryption of data derived from said identity public key and said attribute
3 data, said encryption being according to a second public/private key encryption algorithm
4 using a signature private key, said verifying step comprising:

5 decrypting said digital signature according to said second public/private key
6 encryption algorithm using a signature public key; and

7 comparing the decrypted digital signature to said data derived from said identity
8 public key and said attribute data to verify said descriptor data.

1 139. The television receiving system of claim 134, wherein said first data
2 transformation is an encryption of said source test data and said second data
3 transformation is a decryption of said source test data encrypted by said first data
4 transformation, said first data transformation being performed before said second data
5 transformation.

1 140. The television receiving system of claim 134, wherein said second data
2 transformation is an encryption of said source test data and said first data transformation
3 is a decryption of said source test data encrypted by said second data transformation, said
4 second data transformation being performed before said first data transformation.